[Partial Translation of Document 4]

[Scope of Claims for Patent]

[Claim 1]

A method for encrypting a file in a memory device in an information communication system, comprising a plurality of terminals connected to each other by a communication network and a memory device accessible from said plurality of terminals and shared with a plurality of users, wherein said terminals are connectable by storage media with an operation function distributed to the users in advance, said storage media storing inherent storage medium identifying numbers and a master key list comprised of a plurality of secret numbers; referred to as master keys; writing a file from a terminal to said memory device comprises the steps of

generating a key generating authority list which is a list of said storage medium identification numbers representing a sharer (sharers)of a file to be written and transmitting said key generation authority list from the terminal to the storage medium connected thereto,

selecting a master key based on said received key generation authority list, generating a data key based on said selected master key and said received key generating authority list, and returning the same to said terminal, encrypting a plain text file using said data key to generate an encrypted text file in said terminal, and writing said encrypted text file, said key generating authority list and a file name into said memory device; and reading a file from said storage media by a terminal comprises the steps of

reading the encrypted text file and the key generating authority list from said memory device according to a specified file name,

transmitting said read key generating authority list to the storage medium connected to said terminal,

examining in each terminal whether said received key generating authority list contains its own storage medium identifying number, or if said storage media identifying number contained in said key generating authority list and self storage media identifying number have a predetermined relationship,

selecting a master key based on said key generating authority list, generating a data key based on said selected master key and the received key generating authority list, and returning the same to the terminal when it is detected by said examination step, said received key generating authority list contains its own storage medium identifying number or said storage media identifying number contained in said key generating authority list and self storage media identifying number have a predetermined relationship by said examination, and

decrypting said encrypted text file using said data key to generate a plain text file in said terminal.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-259012
(43)Date of publication of application : 16.09.1994

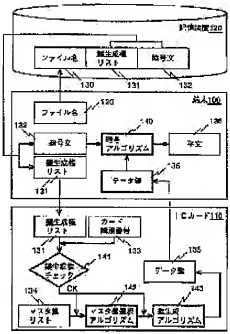
(51)Int.Cl. G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 05-070824
(22)Date of filing : 05.03.1993

(71)Applicant : HITACHI LTD
HITACHI CHUBU SOFTWARE LTD
(72)Inventor : SUZAKI SEIICHI
TAKARAGI KAZUO
MATSUMOTO HIROSHI

(54) ENCIPHERING METHOD BY HIERARCHIC KEY CONTROL AND INFORMATION COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To improve the safety of a file that plural users shares in environment where users are hierarchically sectioned according to kinds of information which can be accessed and to correctly decode a ciphertext file, controlled by a user belonging to one layer, by a user belonging to a layer above the layer.
CONSTITUTION: A terminal 100 reads a key generation right list 131 and a ciphertext 132, making a group with a file name 130 that the user inputs, out of a storage device 120 and sends only the key generation right list 131 to an IC card 110. When the received key generation right list 131 and the card identification number 133 of an IC card 110 satisfy specific relation, the IC card 110 generates a data key 135 on the basis of a master key selected from among the key generation right list 131 and its card master key list 134 and sends the data key to the terminal 100. The terminal 100 decodes the ciphertext 132 with the received data key 135 to generate a plaintext 136.



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号
特開平6－259012
(43)公開日　平成6年(1994)9月16日

(51)Int. Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
G09C 1/00		8837－5L		
H04L 9/06				
9/14				
		7117－5K	H04L 9/02	Z

審査請求　未請求　請求項の数17　FD　(全24頁)

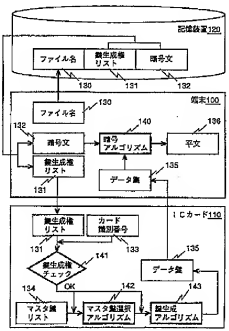
(21)出願番号　特願平5-70824
(22)出願日　平成5年(1993)3月5日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(71)出願人　000233457
日立中部ソフトウェア株式会社
愛知県名古屋市中区栄3丁目10番22号
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　弁理士　矢島　保夫

最終頁に続く

(54)【発明の名称】階層型鍵管理による暗号方法及び情報通信システム

(57)【要約】　(修正有)
【目的】アクセスできる情報の種類によってユーザが階層的に区分される環境において、複数のユーザによって共有されるファイルの安全性を高める。また、ある階層に属するユーザによって管理されている暗号文ファイルを、その上位階層に属するユーザも正しく復号することができる。
【構成】端末１００は、ユーザが入力したファイル名１３０と組になっている鍵生成権リスト１３１及び暗号文１３２を記憶装置１２０より読み取り、鍵生成権リスト１３１だけをＩＣカード１１０に送る。ＩＣカード１１０は、受け取った鍵生成権リスト１３１及び自カード識別番号１３３がある特定の関係を満たすときは、鍵生成権リスト１３１、及び自カードマスタ鍵リスト１３４から選択したマスタ鍵とに基づいて、データ鍵１３５を生成し端末１００に送る。端末１００は受け取ったデータ鍵１３５で暗号文１３２を復号して平文１３６を生成する。



引例3の翻訳箇所

1

【特許請求の範囲】

【請求項1】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

上記記憶装置への、ある端末からのファイルの書き込みは、

書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成し、該鍵生成権リストを、端末からその端末に接続された記憶媒体に、送信するステップと、

該記憶媒体において、受信した鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成するステップと、

該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込むステップとにより行ないことを特徴とする暗号方法。

【請求項2】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう暗号方法であって、

2

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

上記記憶装置への、ある端末からのファイルの書き込みは、

書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成し、該鍵生成権リストを、端末からその端末に接続された記憶媒体に、送信するステップと、

該記憶媒体において、受信した鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成するステップと、

該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込むステップとにより行なうことを特徴とする暗号方法。

【請求項3】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの読出し及び復号を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

あらかじめ上記記憶装置には、複数のユーザによって共有されるファイルのファイル名、当該ファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リスト、及び該鍵生成権リストとに基づいて生成されたデータ鍵で暗号化された暗号文ファイルが、記憶されており、

ある端末による上記記憶装置からのファイルの読出しは、

指定されたファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取るステップと、

読み取った鍵生成権リストを、その端末に接続された記憶媒体に送信するステップと、

該記憶媒体において、受信した鍵生成権リストに自記憶媒体識別番号が含まれているか、またはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にあるか、を検査するステップと、

該検査ステップにより、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかまたはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にある場合は、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成するステップとにより行なうことを特徴とする暗号方法。

基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成するステップとにより行なうことを特徴とする暗号方法。

【請求項４】請求項１ないし３のいずれかに記載の暗号方法において、

前記記憶媒体が、１Ｃカードであることを特徴とする暗号方法。

【請求項５】請求項１または３のいずれかに記載の暗号方法において、

すべてのユーザは、アクセスすることができる情報の種類や重要度によって階層的に区分されているとともに、

前記記憶媒体識別番号は、その記憶媒体を所有するユーザの階層が分かるように設定されており、

前記検査ステップにおける所定の関係は、自記憶媒体識別番号が示す階層が、前記鍵生成権リストに含まれている記憶媒体識別番号が示す階層の上位階層である、という関係であることを特徴とする暗号方法。

【請求項６】請求項１ないし３のいずれかに記載の暗号方法において、

前記記憶媒体識別番号が、その記憶媒体のユーザと他のユーザとの関係を表すことを特徴とする暗号方法。

【請求項７】請求項１または２のいずれかに記載の暗号方法において、

前記記憶装置へのファイルの書き込み時に、データ鍵を生成して端末に返送するステップは、前記受信した鍵生成権リストに自記憶媒体識別番号が含まれているときにのみ、データ鍵の生成と端末への返送を行なうことを特徴とする暗号方法。

【請求項８】請求項５に記載の暗号方法において、

前記記憶媒体中のマスタ鍵リストが、各ユーザ階層毎に異なる秘密数値であるマスタ鍵のうち、その記憶媒体を所有するユーザが属する階層のマスタ鍵及びその下位階層のマスタ鍵によって構成されることを特徴とする暗号方法。

【請求項９】請求項８に記載の暗号方法において、

前記記憶装置へのファイルの書き込み時または読出し時に、前記記憶媒体内部でデータ鍵を生成する場合に、前記鍵生成権リストに記憶媒体識別番号が含まれるユーザが属する階層のうち、最も下位階層のマスタ鍵を選択して使用することを特徴とする暗号方法。

【請求項１０】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されるマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

上記記憶装置への、ある端末からのファイルの書き込みは、

書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成するとともに、該鍵生成権リストの記憶媒体識別番号と所定の関係にある記憶媒体識別番号を算出して該鍵生成権リストに追記し、追記した鍵生成権リストを、端末からその端末に接続された記憶媒体に、送信するステップと、

該記憶媒体において、受信した鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成するステップと、

該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込むステップとにより行ない、

ある端末による上記記憶装置からのファイルの読出しは、

指定されたファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取るステップと、

読み取った鍵生成権リストを、その端末に接続された記憶媒体に送信するステップと、

該記憶媒体において、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかを検査するステップと、

該検査ステップにより、受信した鍵生成権リストに自記憶媒体識別番号が含まれている場合は、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成するステップとにより行なうことを特徴とする暗号方法。

【請求項１１】請求項２に記載の暗号方法において、

前記記憶装置へのファイルの書き込み時の鍵生成権リストの生成の際、書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成するとともに、該鍵生成権リストの記憶媒体識別番号と所定の関係にある記憶媒体識別番号を算出して該鍵生成権リストに追記することを特徴とする暗号方法。

【請求項１２】請求項５に記載の暗号方法において、

前記記憶媒体中のマスタ鍵リストが、各ユーザ階層毎に異なる秘密数値であるマスタ鍵のうち、その記憶媒体を所有するユーザが属する階層のマスタ鍵である階層別マスタ鍵のみによって構成されることを特徴とする暗号方法。

【請求項１３】請求項１２に記載の暗号方法において、

前記記憶装置へのファイルの書き込み時または読出し時

に、前記記憶媒体内部でデータ鍵を生成する場合に、前記鍵生成権リストに記憶媒体識別番号が含まれるユーザが属する階層のうち最も下位階層のマスタ鍵を、前記階層別マスタ鍵から算出して使用することを特徴とする暗号方法。

【請求項１４】請求項１ないし３のいずれかに記載の暗号方法において、

さらに前記各記憶媒体は、その記憶媒体の所有者の個人識別番号を記憶しており、記憶媒体内部でデータ鍵を算出する場合に、該記憶媒体識別番号と個人識別番号とを使って、データ鍵を算出する権利があるかどうかを検査することを特徴とする暗号方法。

【請求項１５】通信網によって相互に接続された複数の端末と、該複数の端末からアクセス可能な記憶装置と、該端末に接続可能であってあらかじめユーザに配布される演算機能を備えた記憶媒体とを備え、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう情報通信システムであって、

上記記憶媒体は、

その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストと、

上記記憶装置へのファイルの書き込み処理において端末から送信された鍵生成権リストを受信し、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送する手段と、

上記記憶装置からのファイルの読出し処理において端末から送信された鍵生成権リストを受信し、該鍵生成権リストに自記憶媒体識別番号が含まれているか、または該鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にあるか、を検査する手段と、

該検査手段により、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかまたは該鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にある場合は、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送する手段とを備え、

上記端末は、

上記記憶装置へのファイルの書き込み処理において、書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成し、該鍵生成権リストを上記記憶媒体に送信する手段と、

上記記憶媒体から返送されたデータ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成する手段と、

該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込む手段と、

上記記憶装置からのファイルの読出し処理において、読出すファイルのファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取る手段と、

読み取った鍵生成権リストを、上記記憶媒体に送信する手段と、

上記記憶媒体から返送されたデータ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成する手段とを備えたことを特徴とする情報通信システム。

【請求項１６】演算手段と、リーダライタインタフェースと、記憶手段とを備え、該記憶手段にはそのＩＣカードに固有のＩＣカード識別番号を記憶したＩＣカードにおいて、

上記リーダライタインタフェースを介してＩＣカード識別番号のリストを受信したとき、該リストに自ＩＣカード識別番号が含まれていたらデータ鍵を生成して出力するとともに、該リストに自ＩＣカード識別番号が含まれていない場合であっても、該リストに含まれているＩＣカード識別番号と自ＩＣカード識別番号とが所定の条件を満足する場合にはデータ鍵を生成して出力することを特徴とするＩＣカード。

【請求項１７】演算手段と、リーダライタインタフェースと、記憶手段とを備えたＩＣカードにおいて、

上記記憶手段には、一般の用途に使用されるカード所有者の個人識別番号のほかに、暗号に使用するための識別番号を記憶していることを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、例えば会社組織のように、アクセスできる情報の種類や重要性によってユーザを階層的に分けることができるような環境において、複数のユーザによって共有される情報を選択的に暗号化することができる暗号方法及びそのような暗号方法を適用した情報通信システムに関し、更に詳しくは、ある階層に属するユーザによって管理されている暗号化された情報を、その上位階層に属するユーザも正しく復号することができる暗号方法及び情報通信システムに関する。

【０００２】

【従来の技術】情報通信機器の発達により、ワークステーションやパソコン等を端末としたローカルエリアネットワーク（ＬＡＮ）が広く用いられるようになってきている。これに伴い、様々な情報が電子化されて送られるようになってきている。

【０００３】ＬＡＮでは、情報は回線上を同報的に流れている。すなわち、情報の送信元は、送信すべき情報に相手先のアドレスを付して回線に送信し、回線上のすべての端末でこれを受信する。受信した端末側では、アドレスを参照して、自己へ向けて送信された情報であるかどうかをチェックする。したがって、ある端末が同報的に送出した情報は、基本的にどの端末でも受信可能である。そのため、機密性の高い情報を送信する場合には、暗号化やアクセス制御といったセキュリティ技術を使っ

て情報の保護を行っている。

【0004】一方、このような環境下では、複数のユーザが共同で作業するために、ファイルの共有といったことも行われる。複数のユーザによって共有されるファイルは各個人毎のファイルと比べて、正しい内容が第三者に漏洩した場合に、その影響が一度に多くのユーザに波及する。したがって、このようにファイルとして蓄積される情報についても、通信回線上を送られる情報と同様に、暗号やアクセス制御といったセキュリティ技術を使って、きちんと保護する必要がある。

【0005】通信回線上を送られる情報を暗号化する場合、あるいはファイルとして蓄積される情報を暗号化する場合には、通信者間、あるいはファイルを共有するユーザ間で暗号鍵を共有する必要がある。

【0006】ところが、ファイルとして蓄積される情報を暗号化する場合には、次のような課題が生じる。

【0007】それは、通信回線上を送られる情報を暗号化する場合は暗号鍵をｌセッション毎に使い捨てにすることができるが、ファイル情報を暗号化する場合には、その暗号文をいつ復号するかわからないので、暗号鍵も暗号文と一緒に保存しておかなければならないということである。

【0008】ファイルを適式に暗号化する方法については、例えば「暗号と情報セキュリティ（編著：辻井　重雄，笠原　正雄；発行：昭晃堂）」に開示されている。

【0009】上記開示例では、まずランダムに生成した乱数でファイルを暗号化して暗号文ファイルを生成する。更に、その乱数もマスタ鍵と呼ばれるシステム固有の秘密数値で暗号化し、暗号文鍵（暗号化された暗号鍵）を生成する。そして、この暗号文鍵を暗号文ファイルとを合わせて記憶しておく。ファイルを読み取る場合には、まず暗号文鍵をマスタ鍵で復号してから暗号文ファイルを復号する。

【0010】その際、暗号文ファイルを復号して正しい内容を読み取る権利があるかどうかのチェックは、別途ファイルのアクセス制御（そのファイルをアクセスする権利がある者かどうかをチェックする方法）によってのみ行っている。

【0011】

【発明が解決しようとする課題】ところで、例えば、図２１のような会社組織では、アクセスできる情報の種類や重要性によってユーザを階層的に区分することができる。このような環境においては、部下の作成したファイルは上司も読み取ることができるが、上司の作成したファイルは部下の側から読み取ることができないようにしたいといった要求がある。

【0012】しかし、上記従来技術では、正しい内容を読み取る権利があるかどうかのチェックをアクセス制御によってのみ行っているので、上司は自分より下位に属するすべての部下のマスタ鍵を知っていなければならない。そうでないと、部下が暗号化したファイルを復号できないからである。しかし、すべての部下のマスタ鍵を管理するのでは、ユーザの負担が大き過ぎる。また、パソコンのようにアクセス制御機能を持たない端末には、適用できないといった問題点がある。

【0013】そこで、本発明の一つの目的は、複数のユーザによって共有されるファイルを、ユーザにあまり負担をかけることなく適式に暗号化して安全性を高めることができる暗号方法及び装置を提供することにある。

【0014】本発明のもう一つの目的は、ある階層に属するユーザによって管理されている暗号文ファイルを、その上位階層に属するユーザも正しく復号することができるような暗号方法及び装置を提供することにある。

【0015】

【課題を解決するための手段】上記目的を達成するため、第１の観点では、本発明は、まず各ユーザに配布された記憶媒体（例えば、ＩＣカード）の識別番号によって、暗号鍵を生成する権利があるかどうかのチェックを行ない、その結果にしたがって暗号鍵を生成することを特徴とする暗号方式を提供する。

【0016】第２の観点では、本発明は、暗号文ファイルを復号する場合に、あらかじめファイル作成者に許可されたユーザかどうかをチェックするだけでなく、そのユーザの上位階層に属するユーザかどうかのチェックをも行なうことを特徴とする暗号方式を提供する。

【0017】第３の観点では、本発明は、暗号鍵生成に使用されるマスタ鍵をユーザ階層毎に用意し、各ユーザに対して、そのユーザが属する階層とその下位階層のマスタ鍵を配布することを特徴とする暗号方式を提供する。

【0018】

【作用】上記第１の観点による暗号方式では、複数のユーザによって共有されるファイルを、ユーザにあまり負担をかけることなく適式に暗号化することができる。

【0019】上記第２の観点による暗号方式では、暗号鍵を生成する権利があるかどうかということを判定する際に、ファイル作成者に許可されたユーザの上位階層に属するユーザかどうかのチェックも行なっているので、ある階層に属するユーザによって管理されている暗号文ファイルを、その上位階層に属するユーザも正しく復号することができる。

【0020】上記第３の観点による暗号方式では、ユーザは自分が属する階層より上位階層のマスタ鍵を手にいれることができないので、ある階層に属するユーザによって管理されている暗号文ファイルを、その下位階層に属するユーザが正しく復号することはできない。

【0021】

【実施例】以下、図面を用いて、本発明の実施例を説明する。なお、以下で説明する図面において、同一の番号は同様の部品・要素を表すものとする。これにより本発

明が限定されるものではない。

【0022】（実施例1）

【0023】図1は、本発明の第1の実施例であり、本発明に係る暗号方法を適用したシステムにおける暗号文（ファイル情報）の復号の手順を示すブロック図である。図2は、本実施例のシステムのシステム構成を示すブロック図である。

【0024】まず、図2を参照して、本実施例のシステム構成を説明する。

【0025】図2において、１００、１０１はワークステーションやパソコン等の端末である。ユーザは、これらの端末を使って種々の作業を行なう。１２０は通信網２１０によって端末１００、１０１と接続された記憶装置である。ユーザは、アプリケーションプログラムを使って作成したファイル等を、この記憶装置１２０に記憶させることができる。また、記憶装置１２０の情報を読出すことができる。

【0026】１１０、１１１は、あらかじめ各ユーザに対してそれぞれ１枚ずつ配布されているＩＣカードである。ユーザは、自己のＩＣカードをリーダライタ２００、２０１に差し込んで、作業を行なう。ＩＣカード１１０、１１１は、リーダライタ２００、２０１を介して、端末１００、１０１とデータのやり取りを行なう。

【0027】図3は、端末１００の内部構成図である。端末１０１など他の端末も同様の構成である。同図に示すように、端末１００は、通信網インタフェース３０１と、リーダライタインタフェース３０２と、ＣＰＵ（中央処理装置）３０３と、表示装置３０４と、入力装置３０５と、メモリ３０６とを有している。それらは、バス３００によって相互に接続されている。

【0028】通信網インタフェース３０１は、通信網２１０を介して記憶装置１２０とデータのやり取りを行なう際のインタフェースである。リーダライタインタフェース３０２は、ケーブル３１０を介してリーダライタ２００との間でデータのやり取りを行なうためのインタフェースである。ＣＰＵ３０３は、演算機能を備え、この端末全体の動作を制御する。表示装置３０４は、ユーザにメッセージを表示するためのディスプレイ等である。入力装置３０５は、ユーザがデータを入力するためのキーボードやマウス等である。メモリ３０６には、通信プログラム３０７、アプリケーションプログラム３０８、およびセキュリティプログラム３０９等が記憶されている。

【0029】メモリ３０６に記憶されている通信プログラム３０７は、記憶装置１２０やリーダライタ２００との間でデータのやり取りを行なう際にそれを制御するプログラムである。アプリケーションプログラム３０８は、ユーザが新規ファイルの作成や既存ファイルの読み取り、書き込み等を行なう際にそれを支援・制御するプログラムである。また、セキュリティプログラム３０９は、ファイルの暗号化及び復号に係る種々の処理を行なうプログラムである。

【0030】図4は、ＩＣカード１１０の内部構成図である。ＩＣカード１１１など他のＩＣカードの構成も同様である。同図に示すように、ＩＣカード１１０は、ＣＰＵ４０１と、リーダライタインタフェース４０２と、メモリ４０３とを有している。それらはバス４００によって相互に接続されている。

【0031】ＣＰＵ４０１は、演算機能を備え、ＩＣカード内の処理の全体を制御する。リーダライタインタフェース４０２は、リーダライタ２００との間でデータのやり取りを行なうためのインタフェースである。メモリ４０３には、通信プログラム４０４、セキュリティプログラム４０５、マスタ鍵リスト４０６、及びカード識別番号４０７等が記憶されている。

【0032】メモリ４０３に記憶されている通信プログラムは、リーダライタ２００との間でデータのやり取りを行なう際にそれを制御するプログラムである。セキュリティプログラム４０５は、リーダライタ２００を介して端末１００から送られてきた情報をもとに暗号鍵を生成する際の種々の処理を行なうプログラムである。

【0033】マスタ鍵リスト４０６は、各ユーザ階層毎に共通の秘密数値であるマスタ鍵のうち、ＩＣカード１１０の所有者が属している階層及びその下位階層のマスタ鍵によって構成される数値列である。

【0034】例えば、本実施例のシステムが適用される組織が、図5のような階層構造であったとする。Ａ，Ｂ，Ｃ，…は組織を構成する各人を示し、上位にいる者が上司である。例えば、Ｊ～Ｐの上司はＦであり、Ｅ～Ｇの上司はＢである。このような組織の場合、第２階層に属するＢが所有するＩＣカードのマスタ鍵リストの構成要素は、ＫＭ２，ＫＭ３，ＫＭ４の三つである。すなわち、ＢのＩＣカードには、自己の階層のマスタ鍵ＫＭ２のほか、下位階層のマスタ鍵ＫＭ３，ＫＭ４も記憶されている。また、第４階層に属するＭのＩＣカードのマスタ鍵リストの構成要素は、ＫＭ４のみである。

【0035】再び図４を参照して、カード識別番号４０７は、ＩＣカード１１０に固有の数値である。全ユーザが役職により図５のように構造化されている場合に、カード識別番号４０７は、ＩＣカード１１０の所有者がどのノードに位置しているかということを示す。

【0036】また、すべてのＩＣカードのカード識別番号は、例えば図６のような識別番号テーブル６００といった形式で記憶装置１２０に記憶される。図６の識別番号テーブル６００において、「氏名」はこの組織に属するＩＣカードを所有するものすべての氏名を示し、「役職」はその者の役職を示す。「個人識別番号」は、その個人に固有の識別番号（例えば、職員番号のようなもの）である。「カード識別番号」は、上記のＩＣカードのカード識別番号４０７の値である。

【００３７】上述したように、カード識別番号によってそのＩＣカードの所有者の組織内における位置（いわば役職）が分かるようになっている。例えば、図５の組織では全体で４階層あるから、図６のようにカード識別番号は４つの数値を並べて構成される。

【００３８】カード識別番号は、左側から順に参照したときに、「０」が出現する位置で、そのカードが属する階層が分かる。例えば、Ａの所有するＩＣカードのカード識別番号は（１，０，０，０）であるが、左側から見て第１番目の数値が「０」以外で「１」、次の第２番目の数値が「０」であるので、Ａは第１階層に属することが分かる。また、Ｇの所有するＩＣカードのカード識別番号は（１，１，３，０）であるが、第１番目の数値が「０」以外で「１」、次の第２番目の数値が「０」以外で「１」、次の第３番目の数値が「０」以外で「３」、次の第４番目に「０」が出現するから、Ｇは第３階層に属することが分かる。

【００３９】さらに、「０」が出現する前までの数値で、組織内の位置が分かる。例えば、Ｃの所有するＩＣカードのカード識別番号は（１，２，０，０）であるが、第１番目の数値「１」でこのカードの所有者が第１階層の第１番目の者（カード識別番号（１，０，０，０）の者）の部下であることが分かる。また、「０」が出現する前にある第２番目の数値「２」で、このカードの所有者がその部下のうちで第２番目の者（すなわち、図５のＣ）であることが分かる。同様にして、例えば、Ｌのカード識別番号（１，１，２，３）により、このＩＣカードの所有者が、カード識別番号（１，１，２，０）の者の部下であって、その部下のうちの第３番目の者であることが分かる。

【００４０】次に、図１を参照して、本実施例において既に記憶装置１２０に記憶されている暗号文（暗号文ファイル）を復号する手順について簡単に説明する。

【００４１】まず、ユーザは、読出したいファイルのファイル名１３０を入力する。端末１００は、ユーザが入力したファイル名１３０を記憶装置１２０に送る。記憶装置１２０は、そのファイル名１３０と組になっている鍵生成権リスト１３１および暗号文１３２を、端末１００へと送る。端末１００は、読み取った鍵生成権リスト１３１および暗号文１３２のうち、鍵生成権リスト１３１だけをＩＣカード１１０に送る。

【００４２】鍵生成権リストとは、当該ファイルを読出し復号する権利のある者を示すカード識別番号のリストである。この実施例では、そのファイルに対するアクセス権を有する者を示すカード識別番号を連結した形式のデータであるが、別の形式で表現してもよい。アクセス権を有する者を示すカード識別番号が分かるようなデータであればよい。鍵生成権リストは、ファイルを作成した者がそのファイルを記憶装置１２０に書き込む際に生成され、記憶装置１２０に書き込まれるようになっている。誰にアクセス権を与えるかは、ファイルを作成した者が指定する。

【００４３】ＩＣカード１１０は、受け取った鍵生成権リスト１３１と自カード識別番号１３３とがある特定の関係を満たすかどうか、鍵生成権チェック１４１を行なう。特定の関係のチェックとは、自カード識別番号１３３が鍵生成権リスト１３１に指定されているかどうか、あるいは自カード識別番号１３３が鍵生成権リスト１３１に指定されている者の上司を示しているかどうか、に関するチェックである。言い換えると、鍵生成権リスト１３１に指定されているアクセス権を有する者であるか、あるいはその上司であるか、をチェックしている。

【００４４】ＩＣカード１１０は、鍵生成権チェック１４１において、鍵生成権リスト１３１と自カード識別番号１３３とが特定の関係を満たすときのみ、マスタ鍵選択アルゴリズム１４２を用いて自カードマスタ鍵リスト１３４からマスタ鍵を選択する。マスタ鍵選択アルゴリズム１４２は、鍵生成権リスト１３１でアクセス権を有すると指定されている者の階層をチェックし、最も下位の階層のマスタ鍵を、マスタ鍵リスト１３４の中から選択する。これは、上位の階層の者のＩＣカードは下位階層のマスタ鍵まで記憶しているのに対し、下位の階層の者のＩＣカードは上位階層のマスタ鍵を記憶していないことによる。すなわち、マスタ鍵を、アクセス権を有する者のうちの最も下位の階層に合せるということである。

【００４５】次に、ＩＣカード１１０は、鍵生成権リスト１３１と選択したマスタ鍵をもとにデータ鍵１３５を生成し、端末１００に送る。

【００４６】端末１００は、受け取ったデータ鍵１３５を用いて、暗号アルゴリズム１４０により暗号文１３２を復号し、平文１３６を生成する。以上のように、平文１３６を得ることができる。

【００４７】次に、図７から図１０を参照して、本実施例におけるユーザの操作や端末１００及びＩＣカード１１０内部の処理について詳しく説明する。

【００４８】図７は、平文ファイルを暗号化して記憶装置１２０に書き込む場合の処理手順を示す流れ図である。

【００４９】本処理は、ユーザが自己のＩＣカード１１０をリーダライタ２００に挿入し、入力装置３０５を使って、アプリケーションプログラム３０８によって作成した平文ファイルを記憶装置１２０に書き込む操作をすることによって開始される（ステップ７００）。

【００５０】端末１００は、まず記憶装置１２０内の識別番号テーブル６００（図６）を読み取り、それを表示装置３０４に表示する（ステップ７０１）。ユーザは、表示された識別番号テーブル６００を参照し、操作した平文ファイルの共有相手を入力装置３０５を使って指定する。端末１００は、その指定されたすべてのユーザの

カード識別番号から成る鍵生成権リストを生成する（ステップ７０２）。そして、その鍵生成権リストをＩＣカードＩＣＣ１１０に送る（ステップ７０３）。

【００５１】ＩＣカードＩＣＣ１１０は、端末１００より送られてきた鍵生成権リストをもとに、データ鍵を生成し、端末１００に送り返す（ステップ７０４）。なお、このＩＣカードＩＣＣ１１０の処理は、図８を参照して後述する。

【００５２】端末１００は、ＩＣカードＩＣＣ１１０より送られてきたデータ鍵を使って平文ファイルを暗号化する（ステップ７０５）。そして、その生成された暗号文ファイルとファイル名と鍵生成権リストとを組にして、記憶装置１２０に書き込む（ステップ７０６）。

【００５３】最後に、ユーザがリーダライタ２００よりＩＣカードＩＣＣ１１０を取り出すことによってすべての処理が終了する（ステップ７０７）。

【００５４】図８は、図７におけるＩＣカードＩＣＣ１１０内部の鍵生成処理（ステップ７０４）を更に詳しく示した流れ図である。本処理は、ＩＣカードＩＣＣ１１０が端末１００より鍵生成権リストを受け取ることによって開始される（ステップ８００）。

【００５５】ＩＣカードＩＣＣ１１０は、まず受け取った鍵生成権リストの構成要素に、自カード識別番号が含まれているかどうか検査する（ステップ８０１）。含まれている場合には、ステップ８０２に進み、処理を続ける。含まれていない場合は、処理を終了する（ステップ８０４）。

【００５６】受け取った鍵生成権リストの構成要素に自カード識別番号が含まれている場合、ＩＣカードＩＣＣ１１０は、その鍵生成権リストを参照し、その構成要素のうち最も下位のユーザ階層に割り当てられているマスタ鍵を、マスタ鍵リストの中から選択する（ステップ８０２）。そして、その選択されたマスタ鍵と鍵生成権リストとからデータ鍵を生成し、それを端末１００に送り返す（ステップ８０３）。そして、すべての処理を終了する（ステップ８０４）。

【００５７】図９は、記憶装置２００に記憶されている暗号文ファイルを読み取り、それを復号する場合の処理手順を示す流れ図である。

【００５８】本処理は、ユーザがＩＣカードＩＣＣ１１０をリーダライタ２００に挿入し、記憶装置１２０に記憶されている暗号文ファイルを読み取る操作をすることによって開始される（ステップ９００）。

【００５９】端末１００は、まず記憶装置１２０に記憶されている各暗号文ファイルのファイル名を読み取り、そのファイル一覧を表示装置３０４に表示する（ステップ９０１）。

【００６０】ユーザは、表示されたファイル名の一覧を参照し、読み込みたいファイル名を入力装置３０５を使って指定する。端末１００は、その指定されたファイル名と組になって記憶されている暗号文ファイルと鍵生成

権リストとを記憶装置１２０から読み取る（ステップ９０２）。そして、鍵生成権リストのみをＩＣカードＩＣＣ１１０に送る（ステップ９０３）。

【００６１】ＩＣカードＩＣＣ１１０は、端末１００より送られてきた鍵生成権リストをもとにデータ鍵を生成し、端末１００に送る（ステップ９０４）。なお、このＩＣカードＩＣＣ１１０の処理は、図１０を参照して後述する。

【００６２】端末１００は、ＩＣカードＩＣＣ１１０より送られてきたデータ鍵を使って暗号文ファイルを復号する（ステップ９０５）。最後に、ユーザがリーダライタ２００よりＩＣカードＩＣＣ１１０を取り出すことによって、すべての処理が終了する（ステップ９０６）。

【００６３】図１０は、図９におけるＩＣカード内部の鍵生成処理（ステップ９０４）を更に詳しく示した流れ図である。図１０の手順は、基本的に図８と同様であるので、同じ処理を行なうステップは同じ番号を付してある。

【００６４】ただし、図１０では、自カード識別番号が、端末１００より受け取った鍵生成権リストに含まれているカード識別番号とある特定の関係を満たす場合にも、データ鍵を生成することを許している点が異なっている（ステップ１０００、１００１）。この場合のある特定の関係とは、ＩＣカードの所有者が、鍵生成権リストにカード識別番号が含まれているユーザの上司であるという関係である。

【００６５】例えば、図６に示すようにカード識別番号が割り当てられている場合、ＩＣカード内のカード識別番号と鍵生成権リストに含まれているカード識別番号とがこの関係を満たすかどうかは、次のようにして検査される。すなわち、ＩＣカード内のカード識別番号と鍵生成権リストに含まれているすべてのカード識別番号との排他的論理和をそれぞれ計算し、ＩＣカードの所有者が属する階層までの数値を検査し、それらがすべて数値０ならば関係を満たしていると判定することができる。

【００６６】これは、ある者（上司）の直属の部下のカード識別番号を、その上司のカード識別番号で左から見て初めて出現する「０」の位置に「１」「２」…を設定して構成するようにしているからである。例えば、図６のＢのカード識別番号（１，１，０，０）とＧのカード識別番号（１，１，３，０）との排他的論理和は（０，０，０，０）となるから、ＢとＣは上司と部下の関係にあると分かる。

【００６７】上述の実施例では、ファイル作成者が指定したユーザ及びそれらユーザとある特定の関係にあるユーザ（例えば、上記で説明した例では上司）が、自分の所有するＩＣカードを端末と接続したリーダライタに挿入した場合にのみ、ＩＣカード内部で正しいデータ鍵が生成される。したがって、ＩＣカードを持たない第三者やファイルを読み取る権利のないユーザは、正しい内容を知ることはできず、共有ファイルの安全性が高くな

る。

【００６８】更に、ファイルを共有するであろう相手毎にあらかじめデータ鍵を共有しておくのではなく、鍵生成権リストやマスタ鍵リストからＩＣカード内部でその都度データ鍵を生成するので、ファイルを共有する相手が多いユーザの負担を軽減し、任意の相手と安全にファイル共有することができる。

【００６９】（実施例２）

【００７０】次に、本発明の第２の実施例を説明する。第２の実施例は、基本的には上述の第１の実施例と同様である。そのシステムのシステム構成、端末の内部構成、およびＩＣカードの内部構成は、上述の第１の実施例の図２，３，４と同様であり、また暗号文（ファイル情報）の復号の手順も図１と同様である。さらに、識別番号テーブルの構成も図６と同様である。

【００７１】上記第１の実施例では、図７の手順によって平文ファイルを暗号化して記憶装置１２０に書き込むが、第２の実施例では図１１の手順を用いる。

【００７２】図１１を参照して、本実施例において平文ファイルを暗号化して記憶装置１２０に書き込む場合の処理手順を説明する。図１１において、図７と同じ処理ステップには同じ番号を付し、説明は省略する。図１１では、ステップ１１００，１１０１が増えている。

【００７３】すなわち、ステップ１１００で、入力装置３０５を使って指定されたユーザのカード識別番号と、ある特定の関係を満たすカード識別番号（例えば、指定されたユーザの上司のカード識別番号）を、端末１００においてあらかじめ生成する。そして、ステップ１１０１で、そのカード識別番号を鍵生成権リストに追加する。追加した結果の鍵生成権リストを、ステップ７０３でＩＣカード１１０に送信するようにしている。

【００７４】また、本実施例において、記憶装置１２０に記憶されている暗号文ファイルを読み取り、それを復号する場合の処理手順は図９と同様である。また、ＩＣカード内部の鍵生成処理は、ファイルの書き込み、読み取りいずれの場合にも図８と同様である。

【００７５】第１の実施例では、ファイルの読出し時に特定の関係をチェックし、例えば上司にもそのファイルが読み出せるようにしていた。これに対し、本実施例では、あらかじめファイルを書き込む際に、特定の関係を満たすカード識別番号、例えば上司カード識別番号を、生成して鍵生成権リストに追加するようにしている。したがって、第１の実施例と同様の効果が得られるほかに、一般的にいって端末より能力の劣るＩＣカード内部での処理を軽減し、より高速化を計ることができる。

【００７６】（実施例３）

【００７７】次に、本発明の第３の実施例を説明する。第３の実施例は、基本的には上述の第１の実施例と同様である。そのシステムのシステム構成、および端末の内部構成は、上述の第１の実施例の図２，３と同様である。識別番号テーブルの構成も図６と同様である。

【００７８】図１２は、本実施例における暗号文（ファイル情報）の復号の手順の概略を示すブロック図である。図１２において、図１と同じ処理あるいは情報には同じ番号を付して説明を省略する。図１２が図１と異なる点は、ブロック１２００，１２１０である。

【００７９】すなわち、本実施例では、ＩＣカード１１０において、マスタ鍵リストから必要なマスタ鍵を選択するのではなく、マスタ鍵生成アルゴリズム１２１０を用いて階層別マスタ鍵１２００から必要とする階層別マスタ鍵を生成するという点が異なる。階層別マスタ鍵１２００とは、当該ＩＣカードの所有者が属する階層のマスタ鍵をいう。例えば、図５の組織では、Ａが所有するＩＣカードは階層別マスタ鍵として第１階層のマスタ鍵ＫＭ１を記憶し、Ｂが所有するＩＣカードは階層別マスタ鍵として第２階層のマスタ鍵ＫＭ２を記憶している。

【００８０】図１３は、階層別マスタ鍵があらかじめ相互に関連付けて生成されており、上位階層のマスタ鍵から下位階層のマスタ鍵を生成できることを示す図である。すなわち、第ｉ階層マスタ鍵１３００から一方向性関数１３１０を用いて第ｉ＋１階層マスタ鍵１３０１を生成することができる。一方向性関数であるから、下位階層のマスタ鍵から上位階層のマスタ鍵を生成することはできない。

【００８１】図１４は、ＩＣカードの内部構成を示すブロック図であり、これは基本的に図４と同じである。ただし、メモリ４０３には階層別マスタ鍵リストではなく、階層別マスタ鍵１４００が一つだけ記憶されている。なお、一方向性関数１３１０はセキュリティプログラム４０５に備えられている。

【００８２】図１５は、ファイルの書き込み及び読み取り時のＩＣカード内部の鍵生成処理を示す流れ図である。これは基本的には図８と同じである。ただし、当カードの階層別マスタ鍵から必要となる階層別マスタ鍵を生成し（ステップ１５００）、その生成された階層別マスタ鍵と鍵生成権リストからデータ鍵を生成する（ステップ１５０１）という点が異なる。

【００８３】また、本実施例におけるファイルの書き込み及び読み取りの際の処理手順は、それぞれ図１１、図９と同様である。

【００８４】本実施例によれば、第１及び第２の実施例と同様の効果が得られるほかに、ＩＣカードに記憶しておかなければならない情報量を減らすことができ、区分されるユーザ階層が多い場合等において有効である。

【００８５】（実施例４）

【００８６】次に、本発明の第４の実施例を説明する。第４の実施例は、基本的には上述の第３の実施例と同様である。そのシステムのシステム構成、および端末の内部構成は、上述の第１の実施例の図２，３と同様である。識別番号テーブルの構成も図６と同様である。

【００８７】図１６は、本実施例における暗号文（ファイル情報）の復号の手順の概略を示すブロック図である。図１６において、図１２と同じ処理あるいは情報には同じ番号を付して説明を省略する。図１２が図１と異なる点は、ブロック１６００，１６１０，１６０１，１６１１である。

【００８８】すなわち、本実施例では、鍵生成権のチェック１４１をする前に、ＩＣカードの所有者が確かに識別番号テーブルに記載されているノード（役職）に位置しているかという使用権のチェック１６１１を行なう点が異なる。

【００８９】図１７は、ＩＣカードの内部構成を示すブロック図であり、これは基本的に図１４と同じである。ただし、メモリ４０３にはその他に、各ユーザごとに異なる数値である個人識別番号１７００が記憶されている。

【００９０】図１８は、本実施例において、平文ファイルを暗号化して記憶装置１２０に書き込む場合の処理手順を示す流れ図である。これは基本的に図１１と同じである。ただし、図１１のステップ７０４が、ステップ１８００，１８０１，１８０２に置き替わっている。

【００９１】図１８において、ステップ７０３で鍵生成鍵リストをＩＣカードに送ると、ステップ１８００でＩＣカードはデータ鍵生成処理１を行なう。これは、後述する図２０のステップ２０００の処理であり、ＩＣカードが自カード識別番号を端末に返送する処理である。

【００９２】端末は、ステップ１８０１で、識別番号テーブル１６００を参照して、ＩＣカードから受け取ったカード識別番号と対応する個人識別番号を探索し、得られた個人識別番号をＩＣカード１１０に返送する。ステップ１８０２で、ＩＣカードはデータ鍵生成処理２を行なう。これは、後述する図２０のステップ２００１以降の処理であり、個人識別番号のチェックやデータ鍵を生成する処理である。

【００９３】図１９は、本実施例において、記憶装置２００に記憶されている暗号文ファイルを読み取り、それを復号する場合の処理手順を示す流れ図である。これは基本的に図９と同じである。ただし、図１８と同様に、図９のステップ９０４がステップ１８００，１８０１，１８０２に置き替わっている。すなわち、識別番号テーブル１６００を参照することにより、ＩＣカードから受け取ったカード識別番号と対応する個人識別番号を探索し、得られた個人識別番号をＩＣカードに返送して、個人識別番号のチェックを行なう点が異なる。

【００９４】図２０は、ファイルの書き込み及び読み取り時のＩＣカード内部の鍵生成処理を示す流れ図である。これは基本的には図１５と同じである。ただし、ステップ２０００，２００１が付け加えられている点が異なる。

【００９５】すなわち、端末から鍵生成権リストを受け取ったら、まず、カード識別番号を端末１００に送る（ステップ２０００）。このステップ２０００は、図１８，１９のステップ１８００に対応する。図１８，１９で説明したように、端末は、ＩＣカードから受け取ったカード識別番号と対応する個人識別番号をＩＣカードに送る。ＩＣカードは、返送されてきた個人識別番号と自カード内の個人識別番号とが一致するかどうかのチェックを行なう（ステップ２００１）。

【００９６】本実施例によれば、第１から第３の実施例と同様の効果が得られるほかに、ユーザが位置するノード（役職）に変更があった場合（このとき、その変更に応じて記憶装置内の識別番号テーブルが書き替えられている）に、以前のユーザにはファイルを復号できなくすることが可能であり、安全性や拡張性を増すことができる。

【００９７】

【発明の効果】以上説明したように、本発明の暗号方式によれば、ファイル共有者を行なうユーザが所有するＩＣカードなどの記憶媒体の識別番号を使って暗号鍵を生成するので、複数ユーザにより共有されるファイルを適式に暗号化することができ、情報の安全性を高めることができる。また、自分より下位階層のユーザのマスタ鍵をすべて持つようにしなくてもよいので、ユーザの素担が軽減される。

【００９８】さらに、上記ＩＣカードなどの記憶媒体の識別番号を、ユーザ階層に即した形で設定しているので、ある階層に属するユーザによって管理されている暗号化された情報を、その上位階層に属するユーザも正しく復号することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示すブロック図である。

【図２】第１の実施例のシステム構成図である。

【図３】第１の実施例における端末の内部構成図である。

【図４】第１の実施例におけるＩＣカードの内部構成図である。

【図５】第１の実施例におけるユーザ及びマスタ鍵の構成図である。

【図６】第１の実施例における識別番号テーブルの構成図である。

【図７】第１の実施例において、平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図８】第１の実施例において、平文ファイルを暗号化する場合のＩＣカード内部の処理を示す流れ図である。

【図９】第１の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

【図１０】第１の実施例において、暗号文ファイルを復号する場合のＩＣカード内部の処理を示す流れ図である。

19

【図１１】本発明の第２の実施例において、平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図１２】本発明の第３の実施例を示すブロック図である。

【図１３】第３の実施例における階層別マスタ鍵の生成方法を示すブロック図である。

【図１４】第３の実施例におけるＩＣカードの内部構成図である。

【図１５】第３の実施例におけるＩＣカード内部の処理を示す流れ図である。

【図１６】本発明の第４の実施例を示すブロック図である。

【図１７】第４の実施例におけるＩＣカードの内部構成図である。

20

【図１８】第４の実施例において、平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図１９】第４の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

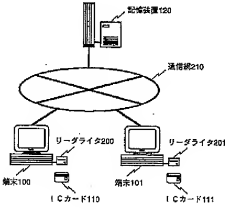
【図２０】第４の実施例におけるＩＣカード内部の処理を示す流れ図である。

【図２１】役職によって階層化されたユーザの構成を示す図である。

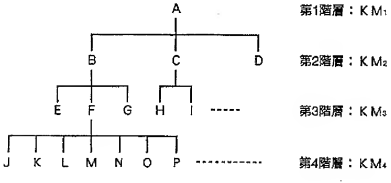
【符号の説明】

１００、１０１…端末、
１１０、１１１…ＩＣカード、
１２０…記憶装置、
２００、２０１…リーダライタ、
２１０…通信網。

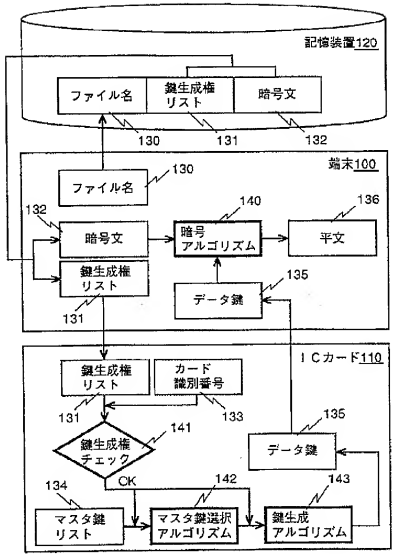
【図２】



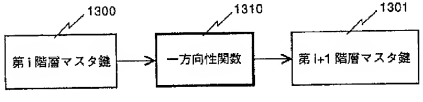
【図５】



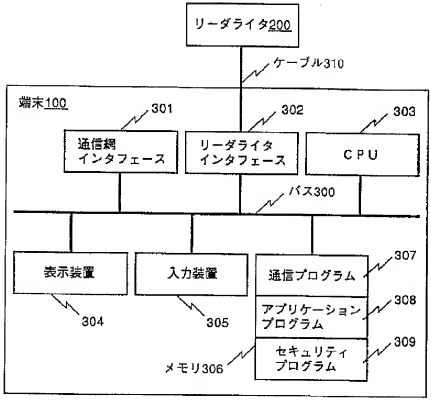
【図１】


記憶装置120
ファイル名
鍵生成権リスト
暗号文
130
131
132
端末100
ファイル名
130
132
暗号文
140
暗号アルゴリズム
136
平文
鍵生成権リスト
131
135
データ鍵
ＩＣカード110
鍵生成権リスト
カード識別番号
131
133
135
データ鍵
141
鍵生成権チェック
CK
142
143
134
マスタ鍵リスト
マスタ鍵選択アルゴリズム
鍵生成アルゴリズム

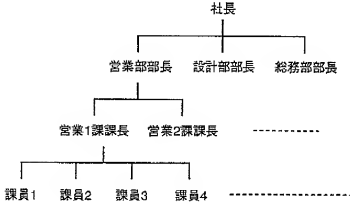
【図１３】


1300
1310
1301
第ｉ階層マスタ鍵
一方向性関数
第ｉ+1 階層マスタ鍵

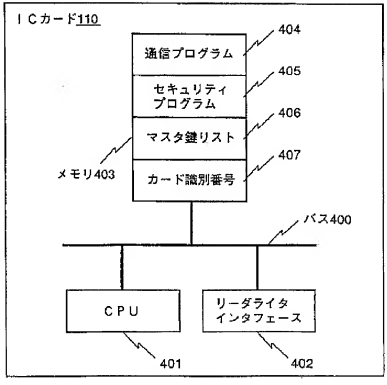
【図3】


リーダライタ200
ケーブル310
端末100
301
302
303
通信網
インタフェース
リーダライタ
インタフェース
CPU
バス300
表示装置
入力装置
通信プログラム
307
アプリケーション
プログラム
308
セキュリティ
プログラム
309
304
305
メモリ306

【図21】


社長
営業部部長
設計部部長
総務部部長
営業1課課長
営業2課課長
課員1
課員2
課員3
課員4

【図4】

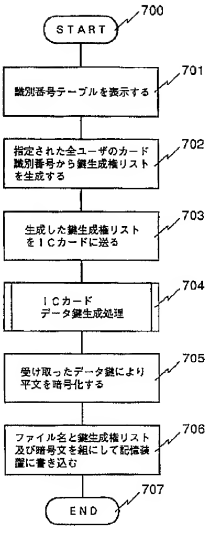

ICカード110
404
通信プログラム
405
セキュリティ
プログラム
406
マスタ鍵リスト
407
カード識別番号
メモリ403
バス400
CPU
リーダライタ
インタフェース
401
402

【図6】

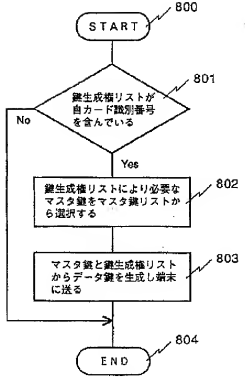
氏名	役　職	個人識別番号	カード識別番号
A	所長	67040m	(1,0,0,0)
B	第1部長	72071m	(1,1,0,0)
C	第2部長	72019m	(1,2,0,0)
⋮	⋮	⋮	⋮
G	第1部第3課長	79001m	(1,1,3,0)
H	第2部第1課長	77038m	(1,2,1,0)
⋮	⋮	⋮	⋮
L	第2部第1課員	89107f	(1,1,2,3)
M	第2部第1課員	90005f	(1,1,2,4)
N	第2部第1課員	90022m	(1,1,2,5)
⋮	⋮	⋮	⋮

識別番号テーブル600

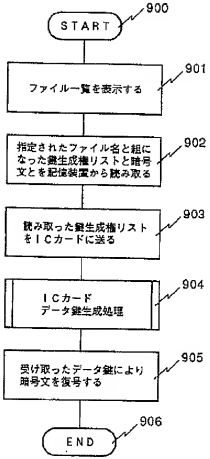
【図7】


START
700
識別番号テーブルを表示する
701
指定された全ユーザのカード識別番号から鍵生成権リストを生成する
702
生成した鍵生成権リストをＩＣカードに送る
703
ＩＣカード
データ鍵生成処理
704
受け取ったデータ鍵により平文を暗号化する
705
ファイル名と鍵生成権リスト及び暗号文を組にして記憶装置に書き込む
706
END
707

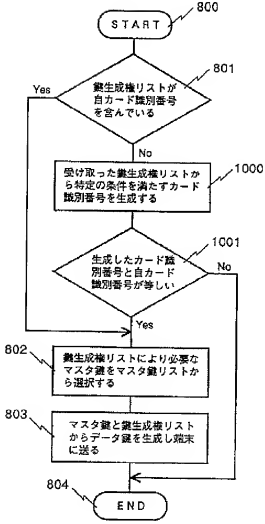
【図8】


START
800
鍵生成権リストが自カード識別番号を含んでいる
801
No
Yes
鍵生成権リストにより必要なマスタ鍵をマスタ鍵リストから選択する
802
マスタ鍵と鍵生成権リストからデータ鍵を生成し端末に送る
803
END
804

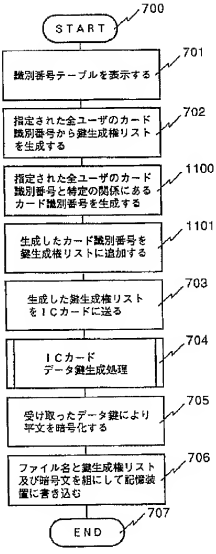
【図9】


START
900
ファイル一覧を表示する
901
指定されたファイル名と組になった鍵生成権リストと暗号文とを記憶装置から読み取る
902
読み取った鍵生成権リストをＩＣカードに送る
903
ＩＣカード
データ鍵生成処理
904
受け取ったデータ鍵により暗号文を復号する
905
END
906

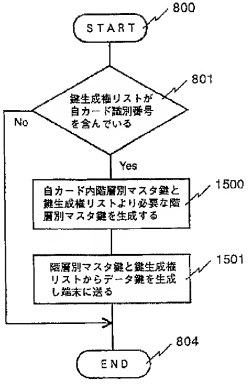
【図10】


START
800
鍵生成権リストが自カード識別番号を含んでいる
801
Yes
No
受け取った鍵生成権リストから特定の条件を満たすカード識別番号を生成する
1000
生成したカード識別番号と自カード識別番号が等しい
1001
No
Yes
鍵生成権リストにより必要なマスタ鍵をマスタ鍵リストから選択する
802
マスタ鍵と鍵生成権リストからデータ鍵を生成し端末に送る
803
END
804

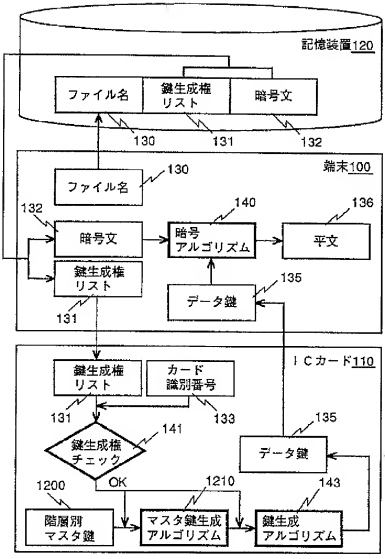
【図１１】


START
700
識別番号テーブルを表示する
701
指定された全ユーザのカード識別番号から鍵生成権リストを生成する
702
指定された全ユーザのカード識別番号と特定の関係にあるカード識別番号を生成する
1100
生成したカード識別番号を鍵生成権リストに追加する
1101
生成した鍵生成権リストをＩＣカードに送る
703
ＩＣカード データ鍵生成処理
704
受け取ったデータ鍵により平文を暗号化する
705
ファイル名と鍵生成権リスト及び暗号文を組にして記憶装置に書き込む
706
END
707

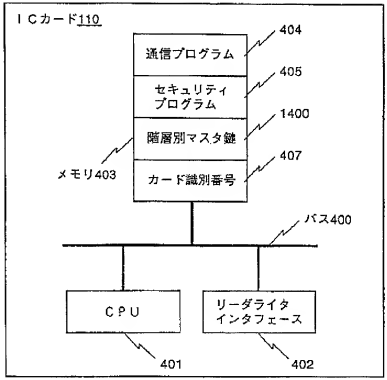
【図１５】


START
800
鍵生成権リストが自カード識別番号を含んでいる
801
No
Yes
自カード内階層別マスタ鍵と鍵生成権リストより必要な階層別マスタ鍵を生成する
1500
階層別マスタ鍵と鍵生成権リストからデータ鍵を生成し端末に送る
1501
END
804

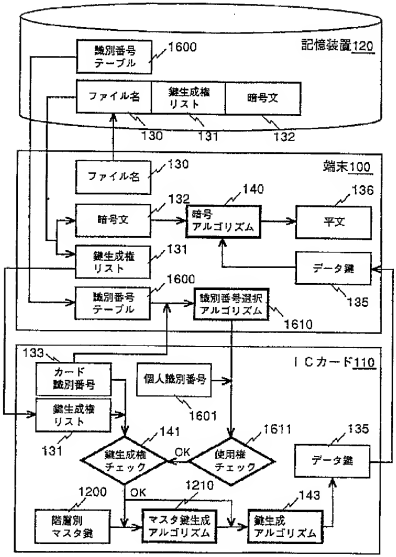
【図12】


記憶装置120
ファイル名
鍵生成権リスト
暗号文
130
131
132
端末100
ファイル名
130
132
暗号文
140
暗号アルゴリズム
136
平文
鍵生成権リスト
131
データ鍵
135
ICカード110
鍵生成権リスト
カード識別番号
131
133
135
141
鍵生成権チェック
データ鍵
OK
1200
1210
143
階層別マスタ鍵
マスタ鍵生成アルゴリズム
鍵生成アルゴリズム

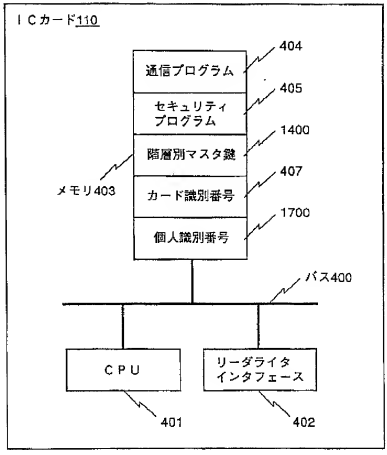
【図14】


ICカード110
404
通信プログラム
405
セキュリティ
プログラム
1400
階層別マスタ鍵
407
カード識別番号
メモリ403
バス400
CPU
リーダライタ
インタフェース
401
402

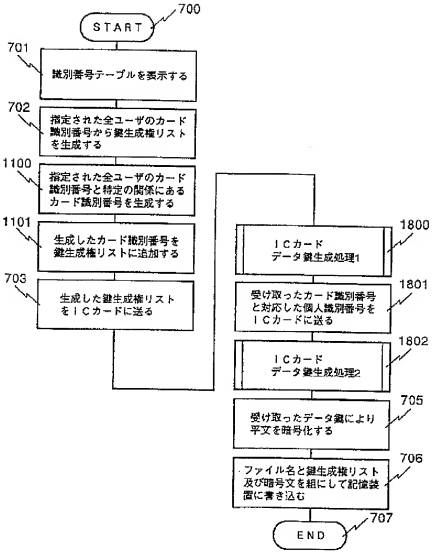
【図16】


識別番号テーブル
1600
記憶装置120
ファイル名
鍵生成権リスト
暗号文
130
131
132
端末100
ファイル名
130
暗号文
132
140
暗号アルゴリズム
136
平文
鍵生成権リスト
131
データ鍵
1600
識別番号テーブル
識別番号選択アルゴリズム
135
1610
133
ICカード110
カード識別番号
個人識別番号
鍵生成権リスト
1601
131
141
鍵生成権チェック
OK
使用権チェック
1611
135
データ鍵
1200
OK
1210
143
階層別マスタ鍵
マスタ鍵生成アルゴリズム
鍵生成アルゴリズム

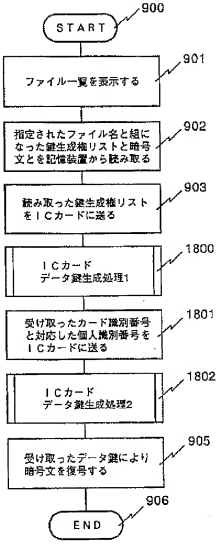
【図17】


ICカード110
404
通信プログラム
405
セキュリティプログラム
1400
階層別マスタ鍵
407
カード識別番号
1700
個人識別番号
メモリ403
バス400
CPU
リーダライタインタフェース
401
402

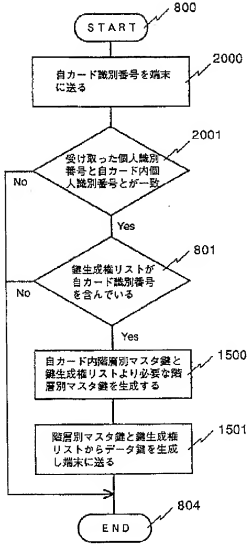
【図１８】


700
START
701
識別番号テーブルを表示する
702
指定された全ユーザのカード識別番号から鍵生成権リストを生成する
1100
指定された全ユーザのカード識別番号と特定の関係にあるカード識別番号を生成する
1101
生成したカード識別番号を鍵生成権リストに追加する
703
生成した鍵生成権リストをＩＣカードに送る
1800
ＩＣカードデータ鍵生成処理1
1801
受け取ったカード識別番号と対応した個人識別番号をＩＣカードに送る
1802
ＩＣカードデータ鍵生成処理2
705
受け取ったデータ鍵により平文を暗号化する
706
ファイル名と鍵生成権リスト及び暗号文を組にして記憶装置に書き込む
707
END

【図19】



【図20】



フロントページの続き

(72)発明者　松本　浩
愛知県名古屋市中区栄三丁目10番22号　日立中部ソフトウェア株式会社内